Communities of Interest in the Net-Centric DoD
Frequently Asked Questions (FAQ)

May 2007
Version 1.1

Prepared by
The Department of Defense
Chief Information Officer
Information Policy Directorate

Index of Questions

Introduction

The DoD Net-Centric Data Strategy outlines the Department's vision for managing data in the Net-Centric environment known as the Global Information Grid (GIG). The Net-Centric goals that drive the Data Strategy focus on empowering users by ensuring all data are visible, accessible, and understandable across the GIG. To achieve the Net-Centric data goals, the Data Strategy acknowledges that there are formal and informal constructs within the Department for managing data. The formal construct uses DoD Issuances, such as directives (e.g. DoD Directive 8320.2) to instruct DoD Components on their responsibilities with respect to achieving the data objectives. Informal collaborative constructs, such as working groups, task forces, and tiger teams contribute greatly to shared information within the Department and therefore will also be used to achieve data objectives. The Data Strategy uses Communities of Interest (COIs) as the general term to describe the collaborative constructs.

The document is written in the "Question and Answer" format to address Frequently Asked Questions (FAQ) pertaining to COIs, and to convey lessons learned in the Department's drive toward Net-Centricity. This "living" document addresses both current and future capabilities envisioned to support COI information sharing activities and will be updated as needed. It will be posted to the COI Toolkit on the Defense Online Portal (https://gesportal.dod.mil/sites/COI%20Information/default.aspx) and the DoD Community of Interest Resources page (http://www.dod.mil/cio-nii/coi/).

NOTE: It is important to note that the scope of this FAQ is limited to COIs and their ***relationship to data activities*** in the Net-Centric DoD environment.

Q1: What is a COI?

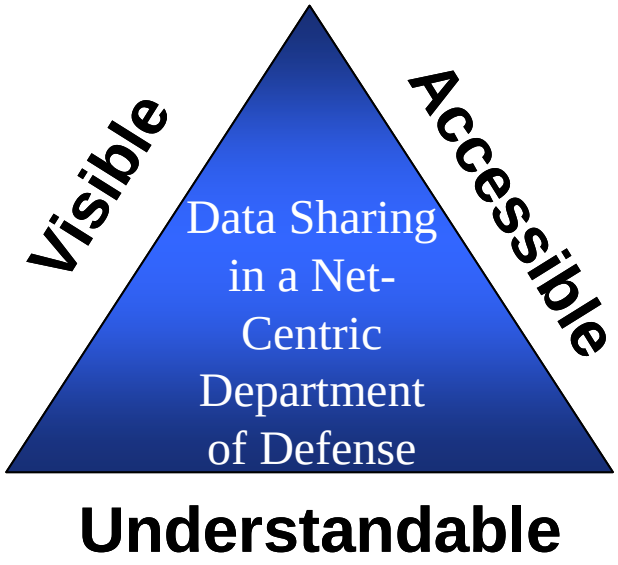
A COI is defined as a collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange[1]. The COI concept is very broad, and covers an enormous number of potential groups of every kind and size. COIs should be joint across DoD Components, non-DoD government agencies and coalition partners

COI membership includes various data owners, producers and consumers that need to share the same semantic knowledge. In addition to DoD components, COI participants may represent organizations outside of DoD (Department of Homeland Security, Department of Transportation, etc.), or allied and coalition partners (NATO, Australia, etc.). The senior leadership of a COI has the latitude to define an appropriate mechanism to manage COI membership. COI membership can be voluntary or mandatory depending on the roles of the participants. A participant's involvement may change throughout the lifecycle of the COI. Initial membership may include the managerial level at the Joint Staff, Military Services, broad OSD representation, selected Defense Agency and Combatant Commands. However, as a COI's effort progresses from the planning stage to a more technical focus, the membership may require greater technical and functional representation. The work of a COI should impact acquisition; therefore, acquisition

[1] DoD Chief Information Officer Memorandum "DoD Net-Centric Data Strategy," *May 9, 20031*

organizations should be encouraged to participate. COIs have the flexibility to engage a range of known participants at various intervals throughout COI lifecycle activities to ensure user requirements are adequately addressed. The chartering process may be a mechanism to solicit the appropriate membership at all levels, as needed.

The Figure below illustrates that COIs exist to make data Visible, Understandable and Accessible.



Data is Visible when it is discoverable by most users, Accessible when it is connected to the network and tools readily exist to use the data, and Understandable when its semantics are well documented.

COIs typically exploit existing resources (data assets) produced and exposed to the enterprise for discovery and reuse. These resources include vocabulary, developed applications, and other data assets.

Q2: Why would a COI form?

A COI is formed to solve a specific information sharing problem and works to resolve data sharing issues affecting the mission of the members (data producers and consumers) that compose the COI. A COI is composed of stakeholders cooperating on behalf of various organizations with emphasis on cross-component activities. COIs exist to increase the sharing of information between known and unanticipated users. COI members should be committed to actively sharing information in relation to their mission and/or task objectives. The functional role of a COI is as an organizational and maintenance construct for enabling information sharing and data standardization. COIs are guided by DoD's strategic goals, existing policies and doctrine. Finally to be fully aligned with the Department's data sharing objective, a COI must recognize the potential for authorized but unanticipated users. It is important that each COI

strive to make their data visible, accessible and understandable to those inside and outside of their community.

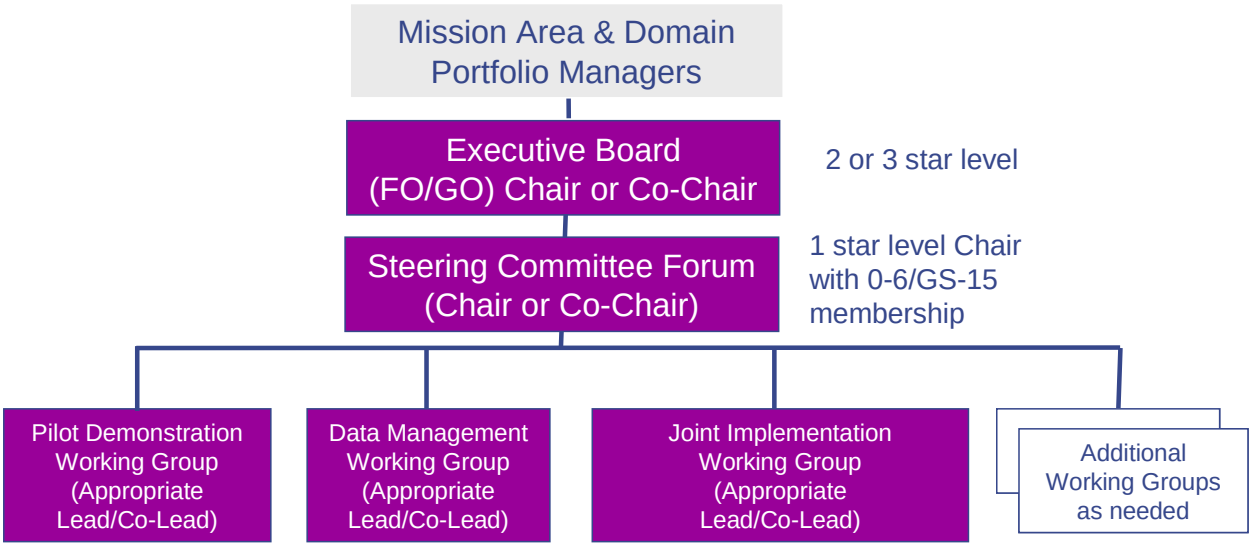
Q3: How are COIs funded?

There is no central pot of "COI funds". DoD Components must continue to budget/plan and manage their resources to support COIs and to expose their data in accordance with the Net Centric Data Strategy (DoD Directive 8320.2) according to the guidance of the Planning, Programming, Budgeting, and Executing (PPBE) processes laid out by the Department".

DoD Directive 5000.2, Operation of the Defense Acquisition System, makes allowance for PoRs to conduct risk reduction efforts whereby pilots/technology demonstrations are done during the Technology Development phase (i.e. before MS B) which allows PoRs to incorporate COI data sources and value-added services in spiral development

Q4: What things should a COI do?

A high level description of the activities a COI should perform are: identify an information sharing problem to solve, define or scope the problem so that a capability solution can be developed 9 to 12 months, identify sources of data that can be leveraged to solve the information sharing problem and marshal the resources required to solve the problem. A suggested starting point for the organizational or governance structure of a COI is illustrated below.



The **Executive Board** of a COI meets as required to promote and endorse COI activities and to get high level buy in for the activities of the COI.

The **Steering Committee** meets on a periodic basis (quarterly and as needed) to ensure the entire COI is aware and agrees to decisions made in the various working groups and to ensure that the appropriate stakeholders participate in the COI work groups. The Steering Committee also coordinates the overall direction of the Pilot Demonstration, Data Management and Joint Implementation Working Groups.

The **Pilot Demonstration Working Group** meets regularly to identify and implement the technical approach to support the information and service sharing capabilities. The primary role of the Pilot Demonstration Working Group is to define the technical approach the COI uses to "expose" their data assets within the COI and across the Enterprise. The data producers participate in this group to ensure that their data are visible and accessible by the unanticipated user who needs it for efficient decision making .

The **Data Management Working Group (DMWD)** defines the shared vocabulary for the COI and implements the shared vocabulary in a schema. The primary role of the Data Management Working Group is to make COI data understandable by developing data structures, data definitions, data models, and other forms of semantic and structural metadata. These products of the Data Management Working Group should be registered in the DoD Metadata Registry for visibility and reuse. In doing so, other communities and users throughout the DoD can find related constructs used to develop systems and to exchange information. By reusing existing metadata, systems and exchange formats tend to require less mediation or transformation. Additionally, by posting metadata to the DoD Metadata Registry, COIs can work together to converge on metadata specifications/standards that support many functions across various communities.

The **Joint Implementation Working Group** defines the high level COI capabilities and recommends the high level schedule for the operational deployment of COI capabilities. They also contributes to a COIs requirements gathering processes, and provides feedback on COI-defined information sharing capabilities

The leadership of a COI has the latitude to merge the Working Groups listed above, add additional Working Groups and make any other changes to the suggested organizational structure above to support the mission and objectives of their COI. The official DoD vision for the activities of a COI are described in Guidance for Implementing Net-Centric Data Sharing (DoD 8320.02-G). The DoD Community of Interest Resources page (http://www.dod.mil/cio-nii/coi/) provides other reference materials.

Q5: What are the criteria for qualifying as a COI?

Any group of producers/consumers who must exchange information and share a vocabulary may form a COI. Members of the COI develop commonality in semantics that allows sharing to take place between the Components. DoD 8320.02-G, Guidance for Implementing Net-Centric Data Sharing encourages COIs to take the initiative in providing the organizational and maintenance construct for data that is to be exchanged. While a COI is the recommended mechanism for making data understandable by defining a common vocabulary and semantics for exchanging information, participation in a COI is not necessarily required in order for a Component to make their data visible or accessible.

Q6: What is the best way for a PoR to expose data?

After the COI has developed a common vocabulary/data model for the COI and registered it in the DoD Metadata Registry, the recommended technical approach for exposing data is to develop

web services which (1) leverage DoD Discovery Metadata Specification (DDMS) to make the PoR's data visible to any authorized user on the GIG in accordance with DoD Directive 8320.2 and Executive Order 13358, and (2) leverage the COI's common vocabulary/data model to exchange data with any authorized consumer on the GIG. COIs are strongly encouraged to leverage DISA's Net-Centric Enterprise Services (NCES) as a core Services Oriented Architecture (SOA) framework to facilitate data visibility and data exchange across the GIG. NCES currently has an Early Capability Baseline (ECB) available on NIPRNET and SIPRNET.

Q7: What are the available NCES services?

The NCES **Content Discovery Service** leverages DDMS to facilitate data visibility. It provides a Federated Search web service specification that PoRs can implement to accept queries and respond with DDMS-compliant discovery metadata records that describe relevant data assets being made visible. DDMS allows for the specification of a URL describing how to access the data asset. This URL could be a direct link to the data asset (for example a Portal/website, a document hosted in a web folder, a servlet that retrieves data from an underlying database and returns it), or a link to a webpage that provides the user with information on what needs to be done in order to access the data asset (for example a webpage containing information on how to subscribe to data that is being published across a particular Messaging bus). DDMS also allows for the specification of security tags in accordance with the Intelligence Community Information Security Markings (IC ISM). Any PoR that implements a Federated Search web service should register that web service endpoint with the NCES Federated Search Aggregator, which provides a single common search interface for any authorized user on the GIG to discover data assets that are being made visible.

Instead of (or in addition to) implementing a Federated Search web service, a PoR may also leverage the NCES **Enterprise Catalog** to make data assets visible via DDMS. This is an NCES-hosted, Enterprise-scalable metadata catalog of DDMS-compliant discovery metadata records that provides web service interfaces for publishing records into the catalog, and removing records from the catalog. The NCES Enterprise Catalog is best suited for data assets that are fairly static in nature, for example the front page of a Portal/website, or a document in a web folder that does not change very often. In addition to federating queries out to registered Federated Search web service endpoints, the NCES Federated Search Aggregator also queries the NCES Enterprise Catalog.

The **NCES Messaging Service** is an Enterprise-scalable Messaging bus that facilitates data exchange by providing web service interfaces compliant with the WS-Eventing specification that allow data producers to publish data across specific channels, and allow data consumers to subscribe to these channels and receive the data being published in an asynchronous (event-driven) fashion. Data may be published in accordance with any XML-based schema(s), allowing each data producer to format the messages in accordance with their COI's vocabulary/data model. Each channel within the NCES Messaging Service contains specific role-based access controls that govern publish and subscribe access.

The **NCES Discovery Service** provides a UDDI interface for making web service endpoints visible to any authorized consumer on the GIG. If a PoR decides to implement a request/response-based web service to exchange data with authorized consumers in accordance with their COI's vocabulary/data model, that web service endpoint should be registered with the NCES Service Discovery Service.

The **NCES Security Services** provide an Enterprise-scalable identity store for maintaining user identities and associated additional attributes (such as roles), as well as an Enterprise-level policy store for maintaining role-based access control policies governing access to specific web services. The NCES Security Services provide the ability for developers to implement web services that restrict users access to only those services and resources that they are entitled to use.

Q8: Are there other considerations when PoR expose data?

A PoR must take into consideration the nature of the data and of the surrounding infrastructure (e.g. processing resources of servers hosting the data, available bandwidth of the surrounding network, etc.) when determining the best mechanism for facilitating data exchange, either via a publish/subscribe mechanism to allow for automated event-driven updates to consumers, or via a request/response-based web service to allow for consumers to periodically poll for updates. There is no "one-size-fits-all" correct answer, but there are certainly aspects to take into consideration. A request/response web service that requires each consumer to poll may work well for exchanging data that does not change very often (for example reports or tasking orders that are only updated every hour or every 24 hours). However if the data is something that may change frequently (for example current position of blue force assets), a request/response-based web service that requires each consumer to poll it could easily result in saturating the surrounding network with traffic if consumers begin polling rapidly (e.g. every second or every 5 seconds) trying to get the most current information. This could also place an unmanageable amount of load on the server hosting the web service if the server does not have the processing resources to handle a high volume of requests. In this case, providing data exchange in an event-driven fashion via a publish/subscribe mechanism may be a better approach. Even when leveraging a publish/subscribe mechanism, similar considerations must be taken regarding the periodicity of publishing. For data that changes frequently, publishing an update the instant a change occurs may also result in saturating the surrounding network with traffic and putting an unmanageable amount of load on both the publisher and the subscribers. In this case, it may be more reasonable to periodically publish updates based upon certain timed intervals (for example every minute or every 5 minutes).

For more information on NCES, please visit the NCES Homepage and the NCES User Workspace on the Defense Online Portal.

Q9: Can a PoR participate in more than one COI?

A Program of Record may participate in more than one COI. The number of COIs a POR participates in is a function of the breathe of the PoRs mission, the number of data sources and data consumers a PoR may require.

Q10: Are PoRs required to expose their data in multiple COI formats?

PoRs that are data producing members of multiple COIs may be required to expose their data in multiple formats. PoRs should work within individual COIs to harmonize data to the greatest extent possible to minimize the publishing of identical data in multiple exchange formats. Tear

line techniques and schema extensions should be leveraged to minimize the need for COIs to support numerous data exchange formats. COIs are encouraged to work together to develop schemas that contain a small set of core data elements that can be leveraged across multiple COIs.

Q11: Are COIs required to use NCES services?

COIs are encouraged to work together to identify the best methods of sharing data within their community. It is strongly recommended that COIs leverage DISA's Net-Centric Enterprise Services (NCES) as a core SOA framework to facilitate discovery by registering existing web service endpoints for each data source in the NCES Service Registry (UDDI), registering the WSDLs and XML Schemas for these web services in the DoD Metadata Registry, and advertising existing Portals/User Interfaces and data assets via the NCES Content Discovery services (Enterprise Catalog and/or Federated Search). The decision not to leverage the DISA's NCES information sharing infrastructure must be made at the Executive Board and/or Steering Committee level.

Q12: How should COIs work within the Portfolio Management process?

Every COI should be aligned with their respective Portfolio Manager to ensure necessary capabilities are in place to facilitate semantic understanding. As an example, a COI may be formally tasked through the sponsoring Portfolio Manager; hence, the COI will need to operate through the Portfolio Management construct of their sponsor(s). Such COIs may have authority from explicit chartering, or implied authority as a result of existing organizational structures.

The intent of the Portfolio Management process is to leverage existing processes for defining, resourcing, and acquiring capabilities against the context of portfolios of related capabilities rather than by platform or program. Portfolio Managers are responsible for ensuring the necessary capabilities to form and operate COIs are planned and programmed for, and assigned to a Domain manager. COIs work through Domain managers from their affiliated Domains to obtain the authority and resources to accomplish their mission. COIs may operate through implied or derived authority; however, if the COIs have a long-term operational focus, then they will likely need to work through their organization's chain of command to find their sponsors.

Specific details on how COIs will operate under the Portfolio Management process are still being finalized. When the details become available, they will be collected and integrated in the COI FAQ.

Q13: Why is a COI pilot's purpose statement limited to a single sentence?

The mission of a COI can be very broad. Each spiral of piloting activity within a COI should be appropriately scoped such that data sharing capabilities can be delivered in a 9-12 month timeframe. The requirement to keep a COI pilot's purpose narrow is designed to ensure that COI members focus only on solving a single problem within each pilot, and to help limit scope the of activities of the COI's Data Management and Pilot Demonstration Working Groups.

Q14: Why are the Data Management and Pilot Demonstration Working Groups partitioned?

The intent of partitioning the activities of the Data Management Working Group and the Pilot Demonstration Working Group is done to (1) recognize the difference in distinct technical skills required to develop shared vocabularies, data models, and schemas within the Data Management Working Group from those required to develop and deploy data sharing services within the Pilot Demonstration Working Group, and (2) to ensure that some activities can occur in parallel to make the most effective use of time. While the separation of these two Working Groups is considered to be a best practice for COIs, it is not a requirement. It is within the authority of the COI Steering committee to organize the COI Working Groups in the best way possible to complete each particular piloting spiral.

Q15: How do you share information securely?

Sharing information securely in a net-centric environment involves the consideration of technical methods for securing access to data and services, as well as the appropriate security policies regarding data access. In general, the COI construct is moving toward a "need-to-share" versus a "need-to-know" environment where data stewards should ensure that their data is discoverable and accessible by any authorized user on the GIG.

There are many different technical approaches for authenticating users and validating their authorization to access certain data assets and services, most of which involve leveraging a local identity store with a local user ID and password to identify each user within each data source. This typically requires each user to have a separate account with a separate user ID and password for each data source, which can quickly become unmanageable. To help resolve this issue and provide a Single Sign-On (SSO) mechanism, the DoD is moving toward a common user identity token across the GIG via the DoD Public Key Infrastructure (PKI), which utilizes an X.509 certificate to identify a user and provide a small set of information about that user. It is recommended that COIs leverage the DoD PKI and allow any X.509 certificate issued by the DoD or any trusted External Certificate Authority (ECA) to be presented for authentication when attempting to access data or services.

Determination of whether or not a user is authorized to access a particular data asset or service depends upon the specific required credentials a user must have in order to be granted access, which are typically governed by existing security policies. Per the DoD PKI, the presentation of a valid DoD or ECA certificate shows that the user is authorized to be on the GIG. The next question to answer is whether or not this is enough to grant the user access, or whether additional credentials must first be verified. The latter case typically requires additional attributes to be associated with a user's identity (e.g. roles, clearance level, etc.) to help qualify additional credentials that the user has (or doesn't have).

One potential technical approach that COIs can take is to leverage the NCES Security Services, which provide:

- A Certificate Validation Service to verify that a certificate was issued by a valid DoD or ECA authority and has not been revoked by the issuing authority.
- A Principal Attribute Service to associate additional attributes (such as roles) with a user's identity.

- A Policy Decision Service allowing for the specification and enforcement of role-based access control policies governing who has the right to access specific methods of a particular web service.

The NCES Security Services currently maintain an Enterprise-level LDAP identity store for maintaining user identities and associated additional attributes (such as roles), as well as an Enterprise-level policy store for maintaining role-based access control policies governing access to specific web services. The need for identity and policy federation is a known item that NCES is planning to address. The COI FAQ will be updated with additional guidance as the NCES Security Services are enhanced to include these capabilities.

For more information on the NCES Security Services, please visit the NCES Homepage and the NCES User Workspace on the Defense Online Portal.